**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA** | : | |
| | : | |
| | : | |
| **v.** | : | **CRIMINAL NUMBER 19-088-1** |
| | : | |
| | : | |
| **NATHAN STEWART WEYERMAN** | : | |

**O R D E R**

**AND NOW**, this day of , 2019, upon consideration of Defendant's Motion to Suppress Evidence Obtained in Violation of the Fourth Amendment, it is hereby **ORDERED** that the Motion is **GRANTED**. The government is hereby **PRECLUDED** from introducing the evidence obtained from Mr. Weyerman's computer and hard drives on September 20, 2018.

**BY THE COURT:**

_____
**THE HONORABLE PAUL S. DIAMOND**
**United States District Court Judge**

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA** | : | |
| | : | |
| | : | |
| **v.** | : | **CRIMINAL NUMBER 19-088-1** |
| | : | |
| | : | |
| **NATHAN STEWART WEYERMAN** | : | |

**DEFENDANT'S MOTION TO SUPPRESS EVIDENCE SEIZED IN VIOLATION OF DEFENDANT'S FOURTH AMENDMENT PROTECTION AGAINST UNREASONABLE SEARCHES AND SEIZURES**

Nathan Weyerman, by and through his attorney, Angela Halim, Assistant Federal Defender, Federal Community Defender Office for the Eastern District of Pennsylvania, respectfully submits this Motion to Suppress evidence obtained as a result of an unreasonable search. As grounds, it is stated:

1. Mr. Weyerman is charged with one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2), (b)(1), and one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)B), (b)(2).

2. The charges stem from a search of Mr. Weyerman's home that he contends was conducted in violation of his Fourth Amendment right against unreasonable searches.

3. Mr. Weyerman owns and operates a General Public License version of lawful peer-to-peer software called 'Freenet'.

4. Freenet is peer-to-peer data sharing software built for anonymity. To retrieve a file from the software, a user must request pieces of that file from other users. The pieces are collected and assembled to create the file intended. Requests are forwarded from peer-to-peer up to eighteen

times. As such, it is difficult to know whether or not the requesting peer is the original requestor of the file, or simply one forwarding a request.

5. The Federal Bureau of Investigation ("FBI") owns and operates a modified version of Freenet which stores information, including IP addresses, of other Freenet users it connects to.

6. The FBI's computer running its version of Freenet received a total of four requests from the same IP address requesting files of child pornography: two on September 18, 2017, one on October 19, 2017, and one on February 1, 2018.

7. Each request had instructions to forward the request a certain amount of times. This number indicated to law enforcement to target the IP address sending the requests. Law enforcement conducted an analysis upon each request using an algorithm. As a result, FBI Agents believed that the IP address was most likely the original requestor for each file.

8. Mr. Weyerman asserts that the FBI's method of determining which requests warrants use of the algorithm is arbitrary and unreliable.

9. The algorithm used by the FBI did not, with sufficient accuracy, determine whether Mr. Weyerman was necessarily the original requestor of the files such that law enforcement officers had probable cause to search Mr. Weyerman's home. The algorithm used makes assumptions about the software which may no longer be true.

10. Law enforcement determined that the IP address requesting the files mentioned above was controlled by Verizon Internet Service Provider. On January 9, 2018, an administrative subpoena was sent to Verizon for subscriber information relating to the IP address. Verizon provided information that the IP address belonged to Nathan Weyerman.

11. On September 20, 2018, law enforcement executed a search warrant on Mr. Weyerman's home and seized Mr. Weyerman's laptop, desktop, and external hard drives.

12. The Fourth Amendment guarantees rights to be free from unreasonable searches and seizures.

13. In order to constitutionally search Mr. Weyerman's home, law enforcement were required to obtain and articulate a basis of probable cause. There was not a sufficient basis for probable cause to search Mr. Weyerman's home.

14. "[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Maryland v. Pringle*, 540 U.S. 366, 370-71 (2003). "To determine whether an officer had probable cause to arrest an individual, we examine the events leading up to the arrest, and then decide "whether these historical facts, viewed from the standpoint of an objectively reasonable police officer, amount to" probable cause." *Id*. The standard "deals with probabilities and depends on the totality of the circumstances." *Id.* at 371.

15. Evidence obtained as a result of an unreasonable search in violation of the Fourth Amendment may be subject to the exclusionary rule. The exclusionary rule is intended to deter police misconduct and protect the privacy rights of individuals; "If exclusion of evidence obtained pursuant to a subsequently invalidated warrant is to have any deterrent effect… it must alter the behavior of individual law enforcement officers or the policies of their departments." *United States v. Leon*, 468 U.S.897, 918 (1984).

16. The Court must balance "the benefits of the rule's deterrent effects against the costs of exclusion, which include 'letting guilty and possibly dangerous defendants go free.' " *United States v. Tracey*, 597 F.3d 140, 151 (3d Cir.2010) (quoting *Herring*, 555 U.S. at 141, 129 S.Ct. 695).

17. Mr. Weyerman asserts that law enforcement did not have a basis of probable cause to search his home or his electronic devices on September 20, 2018.

18. This case presents this Court an opportunity to protect individuals from unreasonable searches in a relatively new field. Mr. Weyerman has been unable to locate any precedential authority on the issue of whether this specific algorithm and law enforcement's methodology is strong enough to support a finding of probable cause.

**WHEREFORE**, for the reasons set forth in the accompanying Memorandum of Law, as well as any which may become apparent at a hearing or the Court deems just, Defendant Nathan Weyerman, by his counsel undersigned, respectfully requests that the Court grant his Motion and preclude the government from introducing all evidence seized on September 20, 2018.

Respectfully submitted,

/s/ Angela Halim
ANGELA HALIM
Assistant Federal Defender

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA** | : | |
| | : | |
| | : | |
| **v.** | : | **CRIMINAL NUMBER 19-088-1** |
| | : | |
| | : | |
| **NATHAN STEWART WEYERMAN** | : | |

**MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS EVIDENCE SEIZED IN VIOLATION OF DEFENDANT'S FOURTH AMENDMENT PROTECTION AGAINST UNREASONABLE SEARCHES AND SEIZURES**

Defendant Nathan Weyerman is charged in a grand jury indictment with one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2), (b)(1), and one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)B), (b)(2). The charges stem from a search of Mr. Weyerman's computer that he contends was conducted in violation of his Fourth Amendment right against unreasonable searches. Law enforcement received four partially anonymous requests for media files containing child pornography through a peer-to-peer data sharing software. The FBI used an algorithm to determine the probability of whether the anonymous requestor was the original source of the request, and concluded that it most likely was. That algorithm, alone, is insufficient to warrant a finding of probable cause; therefore, the subsequent search was conducted in violation of the Fourth Amendment. The defense moves to exclude all evidence obtained as a result of the search from introduction into evidence at trial.

## I. BACKGROUND

Mr. Weyerman owns and operates a General Public License version of a peer-to-peer software called 'Freenet'. Freenet software is a peer-to-peer data sharing software built for anonymity and censorship free communication, wherein users, or 'peers', upload files that are

broken down into chunks and stored on multiple other peer computers. To retrieve a file from the software, a user must request pieces of that file from other users which are collected and assembled to create the file intended. Requests are forwarded from peer to peer up to eighteen times to gather all the necessary pieces. As such, it is difficult to know whether or not a requesting peer is the original requestor of the file, or simply one forwarding a request made by another peer.

The Federal Bureau of Investigation ("FBI") owns and operates a modified version of Freenet which stores information, including IP addresses, of other Freenet users. The FBI computer running its version of Freenet received a total of four requests from the same IP address requesting files of child pornography: two on September 18, 2017, one on October 19, 2017, and one on February 1, 2018. Law enforcement conducted an analysis upon these requests, using an algorithm to make a determination whether the IP address requesting the subject files was the original requestor or a forwarding requestor. As a result, FBI Agents came to believe that the IP address was most likely the original requestor for each file and used this algorithm as the basis for probable cause.

Law enforcement concluded that the IP address requesting the files mentioned above was controlled by Verizon Internet Service Provider. On January 9, 2018, an administrative subpoena was sent to Verizon for subscriber information relating to the IP address. Verizon provided information that the IP address belonged to Nathan Weyerman. On September 20, 2018, law enforcement executed a search warrant at Mr. Weyerman's home and seized his laptop, desktop, and external hard drives.

## II. DISCUSSION

There is no bright line rule for probable cause; the Supreme Court has "rejected rigid rules, bright-line tests, and mechanistic inquiries in favor of a more flexible, all-things-considered approach." *Florida v. Harris*, 568 U.S. 237, 244 (2013). However, courts' interpretations of what evidence *is* sufficient for probable cause are extensive and instructive. The process and algorithm by which the FBI identified Mr. Weyerman's IP address and concluded that he was likely the original requestor does not rise to the level of probable cause justifying a search of his home and electronic devices.

### A. Legal Standard

The Fourth Amendment guarantees an individual's right to be free from "unreasonable searches and seizures." U.S. Const. Amend. IV. Absent a finding of probable cause supporting a valid search warrant, the search of Mr. Weyerman's home and/or electronic devices was unconstitutional. In this case, Agents did obtain a search warrant after submitting an Affidavit of Probable Cause authored by FBI Agent Rebecca A. Quinn. *See* Exhibit A, attached hereto.

"[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Maryland v. Pringle*, 540 U.S. 366 (2003). 370-71. "To determine whether an officer had probable cause to arrest an individual, we examine the events leading up to the arrest, and then decide "whether these historical facts, viewed from the standpoint of an objectively reasonable police officer, amount to" probable cause." *Id*. The standard "deals with probabilities and depends on the totality of the circumstances." *Id.* at 371.

The algorithm used by the FBI did not, with sufficient accuracy, determine whether Mr. Weyerman's IP address was actually the original requestor of the files such that agents had

probable cause to search his home. This case presents this Court an opportunity to protect individuals from unreasonable searches in a relatively new field. Mr. Weyerman has been unable to locate any precedential authority on the issue of whether this specific algorithm is strong enough to support a finding of probable cause.

**B. Freenet Background**

"Freenet is a platform for censorship-resistant communication and publishing. It is designed to ensure true freedom of communication over the Internet." The Freenet Project, *About*, (2019) https://freenetproject.org/pages/about.html. "Communications by Freenet nodes are encrypted and are routed through other nodes to make it extremely difficult to determine who is requesting the information and what its content is. Users contribute to the network by giving bandwidth and a portion of their hard drive (called the "data store") for storing files." *Id*.

Freenet is a legal tool for the free exchange of information. The creators of Freenet address any question of legality head on. On the Freenet website, the creators have included language that reads

> We don't currently know of any prosecutions for merely using Freenet…ACTA [Anti-Counterfeiting Trade Agreement] might have wide-ranging effects, including on Freenet, should it pass… There have also been attempts to force peer to peer systems to provide wiretapping capabilities in the USA, and there are worrying developments in the UK that might result in it being blocked, but not being made illegal per se. As far as we know none of these things… have passed. Many of these are arguable either way (depending on how broadly the legislation is applied) and will have to be decided in caselaw.

The Freenet Project, *Help*, (2019) https://freenetproject.org/pages/help.html. The creators make it clear that they did not intend for any illegality to be connected to their software. They state that

> We have done everything we can to make it extremely difficult for any sane legal system to justify punishing someone for running a Freenet node, and there is little precedent for such action in today's developed countries. Many legal systems recognize the importance of freedom of speech, which is Freenet's core goal.

*Id*. The process by which Freenet operates is described below:

> Users contribute to the network by giving bandwidth and a portion of their hard drive (called the "data store") for storing files. Files are automatically kept or deleted depending on how popular they are, with the least popular being discarded to make way for newer or more popular content. Files are encrypted, so generally the user cannot easily discover what is in his datastore, and hopefully can't be held accountable for it.

The Freenet Project, *About*, (2019) https://freenetproject.org/pages/about.html. Therefore, in order to retrieve files, a user must send out a request to collect and assemble pieces of that file from other user's data store.

### C. The Indicator Used by Law Enforcement to Trigger Running of the Algorithm is Unreliable

As discussed above, Freenet retrieves files by sending out requests from a user to its peers to collect pieces of that file. That user's peers then forward the request for file pieces to their own sets of peers. The number of times a request can be forwarded is called the Hops to Live, or 'HTL'. The default maximum HTL is 18. Freenet hides the identity of the original requestor of a file by randomizing when the HTL of a request is forwarded as 17 or 18. A randomized HTL value is made for each peer-to-peer connection, not for the request as a whole. A peer receiving the original request forwards the randomized HTL value to the next node, which in turn forwards the request again, decrementing the HTL as it travels down a path.

The source code for Freenet is publicly available. The source code developed for rerouting each request, and how the process, called probabilistic decrement, works reads:

```
/**
     * Decrement the HTL (or not), in accordance with our
     * probabilistic HTL rules. Whether to decrement is determined once for
     * each connection, rather than for every request, because if we don't
     * we would get a predictable fraction of requests with each HTL - this
     * pattern could give away a lot of information close to the originator.
     * Although it's debatable whether it's worth worrying about given all
     * the other information they have if close by ...
     * @param htl The old HTL.
     * @return The new HTL.
     */
    public short decrementHTL(short htl) {
            short max = node.maxHTL();
```

```
if(htl > max)
        htl = max;
if(htl <= 0)
        return 0;
if(htl == max) {
        if(decrementHTLAtMaximum || node.disableProbabilisticHTLs)
                htl--;
        return htl;
}
if(htl == 1) {
        if(decrementHTLAtMinimum || node.disableProbabilisticHTLs)
                htl--;
        return htl;
}
htl--;
      return htl;
```

Noting the included comment, the HTL is determined for each connection to a peer; the HTL is not the same for every peer that receives a part of the original request. As such, a peer may receive a number of different values. A receiving peer, forwarding an original request, may send out the request to its own set of peers with an HTL of 16 (if the peer received an HTL 17 request and decremented it), 17 (if the peer received an HTL 17 or 18 request and chose to decrement or not), or 18 (if the peer is just forwarding the original request without any decrement). Therefore, if law enforcement were to "receive a number of file requests with HTL values of 16 or 17 mixed with HTL 18s for the same file, it means HTL 18s are the result of randomly not decrementing the HTL and the subject IP is not the requestor." Missouri ICAC Task Force, *Black Ice: The Law Enforcement Freenet Project*, (September 2013) https://retro64xyz.gitlab.io/assets/pdf/blackice_project.pdf. (Attached hereto as Exhibit B.)

Conversely, "a number of HTL 18s for a file without any HTL 16/17s makes it highly likely that [the] subject is the requestor." *Id*.

The affidavit of probable cause states that "only those requests that were intended for law enforcement computers as recipients, that are forwarded 17 or 18 times, and are associated with a file of interest are analyzed." Affidavit of Probable Cause ¶ 28. The first issue with this is that

the affidavit gives no information on whether there were other requests from Mr. Weyerman's node with HTL values of 16 as well. As stated above, this would mean that the requests with values of 18 were the result of randomly not decrementing the original value.

Further, the selection of requests with HTL values of 17 and 18 is also an unreliable method. As stated, an HTL value of 17 is unlikely to come from the original requestor. It could be a decremented request from the original requestor, a forwarded request from a first-round peer, or even a forward from a second-round peer, thus three levels away from the origin. The probabilistic decrement keeps the true source unknown to the receiving peer.

In order to determine the true requestor, a law enforcement computer would need to establish the HTL value of requests received and be able to track backwards to the source. However,

> [s]ince the only IP addresses known to the LEFnode [Law Enforcement node] are the ones directly connected to it, there is currently no way to tell what IP requested a key if the HTL is less than 18… There is also the possibility that a request with a HTL of 18 is not from the originator but randomly (50/50 chance) passed along without being decremented. A feature, called probabilistic HTL, will change the HTL when at 18, or not decrement it, as it reroutes the request.

*Id*. This means that the law enforcement node has no way to track the IP addresses of the nodes that have forwarded the request. The only information law enforcement has is that they received a request from this specific IP address, with no history of where the request may have come from before that.

Further, these HTL values that law enforcement used as a red flag may be completely arbitrary. "It is possible to change the max or starting HTL within the configuration screens for Freenet." Missouri ICAC Task Force, *Black Ice: The Law Enforcement Freenet Project*, (September 2013) https://retro64xyz.gitlab.io/assets/pdf/blackice_project.pdf. As such, the HTL

number can be changed depending on the user's preference. A user could potentially set the HTL of a request to 20, contacting the law enforcement node three to five reroutes away from the original request.

The potential for the peer sending the FBI the request to be the original requestor is also lowered when typical Freenet traffic is factored in. Requests for child pornography related documents accounts for 35% of all Freenet traffic. Brian Levine, Marc Liberatore, Brian Lynn, Matthew Wright, *Statistical Detection of Downloaders in Freenet*, (2017) (Attached hereto as Exhibit C.) With such a high volume of requests for child porn related documents, and those requests being forwarded multiple times, the chance for an IP address to unknowingly forward a request for child porn is high.

Therefore, Mr. Weyerman asserts that the HTL indicator that triggered this investigation is an unreliable method of selecting targets. The FBI has placed an undue amount of reliance on the reroute requests. Considering the randomized nature of HTL's, it is clear that the process of the probabilistic decrement barricades peers from tracing the request backward. Not only is this an unreliable indicator of closeness to the origin, but the affidavit did not provide a complete picture of whether or not other requests with different HTLs were received. As such, using this value as a method to decide which IP addresses to target is too broad.

**D. The Algorithm Used by the FBI Makes Invalid Assumptions**

After receiving requests for pieces of child pornography related files from an IP address, the FBI ran an algorithm to determine the probability that those requests came from the original requestor. This algorithm uses two factors to make this determination: the fraction of the file requested, and the number of peers a requestor shares that request with. The assumption made by this test is that the further down the line of requests, the smaller the fraction is. This is true; a

forwarding peer does in fact equally divide the request among its own peers. For example, if a node with three peers of its own were to receive a request for 30 kilobytes, it would forward that request to its peers asking for 10 kilobytes from each.

There are a few problems with this type of algorithm. First, the "peer reviewed article" mentioned in ¶ 29 of the Affidavit of Probable Cause that "finds that a formal mathematical formula based on this reasoning is highly accurate" makes a stale, incorrect assumption. In the aforementioned article, the authors state that the "minimum number of allowable peers is 10." Brian Levine, Marc Liberatore, Brian Lynn, Matthew Wright, *Statistical Detection of Downloaders in Freenet*, (2017). However, this article was written in 2017; since then, Freenet has allowed users to configure their peer settings and specifically set the amount of peers they connect with to be between 0 and 40. Freenet, *Opennet Configuration*, (2019) http://freenet.makdisse.com/current/opennet.html. The test of the algorithm may no longer be accurate.

Further still, the law enforcement node is not able to see how many peers the previous forwarding node(s) had. As such, the variable is extremely skewed. The affidavit states that

> In basic terms, the methodology relies on two primary facts about the Freenet software: first, the original requestor divides up its requests for pieces of a file among its peers, sending a roughly equal fraction of the requests to each peer; second, if a peer does not have the requested pieces, the peer takes the fraction of requests for pieces of a particular file and divides them up again among its own peers. Because a peer that is merely routing another peer's request would ask its peers for a significantly smaller portion of the pieces of a file than an original requester, it is possible for the recipient of requests to determine whether a request is significantly more ·likely than not from an original requester.

Affidavit of Probable Cause, ¶29. If, for example, two previous nodes only had one or two peers, then the fraction of the file size would still be fairly large, as the nodes would essentially be forwarding the same size piece of the file that was requested of them.

The files allegedly requested by Mr. Weyerman's IP address were videos with relatively large sizes. If those requests were only being forwarded by Mr. Weyerman's node from another node with a limited number of peers, then there is a large chance for a false positive. The algorithm makes the assumption that the larger the requested piece of the file, the better chance of the original requestor. Therefore, not only is the trigger for the analysis unreliable, the algorithm itself is subject to false results.

## III. CONCLUSION

For all the reasons set forth above, the evidence obtained on September 20, 2018 is not admissible under the Fourth Amendment to the Constitution. Mr. Weyerman, by his counsel undersigned, respectfully requests that the Court grant this Motion and preclude the government from introducing the contested evidence.

Respectfully submitted,

/s/ Angela Halim
ANGELA HALIM
Assistant Federal Defender

**CERTIFICATE OF SERVICE**

I, Angela Halim, Assistant Federal Defender, Federal Community Defender Office for the Eastern District of Pennsylvania, hereby certify that I have caused a copy of Defendant's Defendant's Motion to Suppress Evidence Obtained in Violation of the Fourth Amendment, and Memorandum of Law in Support Thereof, to be filed and served electronically through the Eastern District of Pennsylvania's Electronic Case Filing ("ECF") system, upon Seth M. Schlessinger, Assistant United States Attorney, whose office is located at 615 Chestnut Street, Suite 1250, Philadelphia, Pennsylvania 19106.

/s/ Angela Halim
ANGELA HALIM
Assistant Federal Defender

DATE: October 9, 2019